WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

receiving a call from an application via an application programming interface, the call having parameters for a connection to an endpoint that the application desires to establish;

receiving an indication from the application that the application desires to establish the connection; and

making a call to a firewall to establish the connection in accordance with the parameters.

2. The method of claim 1, further comprising, at the firewall, evaluating the parameters with respect to a policy and, if the parameters meet the policy, establishing the network connection in accordance with the parameters.

3. The method of claim 1, wherein the parameters comprise a known endpoint to which the application would like to be connected.

4. The method of claim 3, wherein the parameters further comprise a request to limit the connection to a single connection.

5. The method of claim 4, further comprising, after the connection has been established, closing the connection in accordance with the request.

6. The method of claim 1, wherein the parameters comprise a request for bandwidth of connection throttling for the connection.

7. The method of claim 1, wherein the parameters comprise limiting the connection to a subset of interfaces, local addresses, or remote addresses, or combinations thereof.

8. The method of claim 1, wherein the parameters comprise a timeout policy for the connection.

9. The method of claim 1, wherein the parameters comprise turning off or on specific protocol options.

10. The method of claim 1, wherein the parameters comprise information about a property of a flow that requires special handling.

11. The method of claim 10, wherein the information comprises a request for authentication or encryption.

12. The method of claim 1, wherein the indication comprises opening a listening socket.

13. The method of claim 1, wherein the indication comprises connecting to a socket.

14. The method of claim 1, wherein the call to the firewall is made via a firewall application programming interface.

15. The method of claim 1, wherein the firewall is located on a computer with the application.

16. The method of claim 1, wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information to the edge firewall about the connection.

17. The method of claim 1, wherein the firewall comprises an edge firewall, and further comprising an

authenticated protocol to communicate information to the edge firewall about the connection.

18. A computer-readable medium having computer-executable instructions for performing the method recited in claim 1.

19. A computer system comprising:

an operating system;

an application programming interface associated with the operating system and configured and adapted to receive a call from an application, the call having parameters for a connection to an endpoint that the application desires to establish; and

an enforcement module associated with the operating system and configured and adapted to:

receive an indication from the application that the application desires to establish the connection; and

make a call to a firewall to establish the connection in accordance with the parameters.

20. The computer system of claim 19, further comprising a firewall application programming interface for making the call to the firewall.

21. A computer-implemented method, comprising:

establishing policies for connections to endpoints;

receiving a connect attempt, a listen attempt, or a combination thereof from an application or a service;

extracting user and application or service information from the connect attempt, the listen attempt, or the combination thereof;

evaluating the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof complies with the policies; and

if the connect attempt, the listen attempt, or the combination thereof complies with the policies, configuring the firewall to allow the connect attempt, the listen attempt, or the combination thereof.

22. The method of claim 21, further comprising if the connect attempt, the listen attempt, or the combination thereof does not comply with the policies, sending a notification to a user of the application or service.

23. The method of claim 22, wherein the notification comprises a selection to allow the connection.

24. The method of claim 21, wherein establishing the policies comprises receiving a policy from the application or service.

25. The method of claim 24, wherein receiving policies comprises receiving policies via an application programming interface.

26. The method of claim 24, wherein the policy received from the application or service comprises inbound or outbound restrictions using one or more Internet Protocol addresses, information about a subnet, information about scope of the connection, or combinations thereof.

27. The method of claim 24, wherein the policy received from the application or service comprises communication security level.

28. The method of claim 27, wherein the communication security level comprises authentication.

29. The method of claim 27, wherein the communication security level comprises encryption.

30. The method of claim 21, wherein the firewall comprises a host firewall located on a computer with the application.

31. The method of claim 21, wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information about the connection.

32. The method of claim 21, wherein the firewall comprises an edge firewall, and further comprising an authenticated protocol to communicate information to the edge firewall about the connection.

33. A computer-readable medium having computer-executable instructions for performing the method recited in claim 21.

33. A computer system, comprising:

a firewall; and

an interception module configured and adapted to:

access policies for applications, services, or combinations thereof regarding connections to endpoints;

intercept a request for a connect attempt, a listen attempt, or a combination thereof from an application or a service;

extracting user and application or service information from the connect attempt, the listen attempt, or the combination thereof;

evaluate the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof complies with the policies; and

if the connect attempt, the listen attempt, or the combination thereof complies with the policies, instruct the firewall to configure the connect attempt, the listen attempt, or the combination thereof.

34. The computer system of claim 33, wherein the interception module comprises a policy cache for storing the policies.

35. The computer system of claim 33, wherein the interception module comprises an application programming interface for receiving the policies from an application or service.

36. The computer system of claim 33, wherein the interception module comprises a firewall client for communicating information about the connect attempt, the listen attempt, or the combination thereof to an edge firewall.